#3

62478-1800

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Examiner:
Makoto Tatebayashi et al.	Group Art Unit: ~~2776~~ 2132
Serial No.: 09/638,616	Official
Filed: August 15, 2001	RECEIVED (6-27-03)
For: ENCRYPTION METHOD, ENCRYPTION APPARATUS, DECRYPTION METHOD, AND DECRYPTION APPARATUS	June 27, 2003 Irvine, California

PETITION TO MAKE SPECIAL

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

In accordance with MPEP Section 708.02(viii), applicant hereby requests that the above-identified application be made special and a fee required in accordance with 37 C.F.R. Section 1.17(i) is submitted herewith.

A European Search Report on a corresponding European Application No. 00306872.3 has been conducted and the following references were cited:

EP 0 874 496 A (MATSUSHITA ELECTRIC INDUSTRIAL CO. LTD.) 28 October 1998 (1998-10-28)
the whole document

STALLINGS WILLIAMS: "Cryptography and network security: principles and practice - 2nd ed"
CRYPTOGRAPHY AND NETWORK SECURITY, XX, XX, 1999, XP002193563
ISBN: 0-13-869017-0
page 61-page 62

Received from < 949 955 2507 > at 6/27/03 3:02:19 PM [Eastern Daylight Time]

CHARNES C; O'CONNOR L; PIEPRZYK J; SAFANI-VAINI R; ZHENG Y:
"Comments on Soviet encryption algorithm"
ADVANCES IN CRYPTOLOGY-EUROCRYPT '94, PERUGIA, ITALY. SPRINGER VERLAG., 12 MAY 1994 (1994-05-12), pages 433-438, XP002193564
ISBN: 3-540-60176-7
abstract
page 434, paragraph 3 - page 435, paragraph 1

Received from < 949 955 2507 > at 6/27/03 3:02:19 PM [Eastern Daylight Time]

Remarks

The Ohmori EP application is directed to cryptographic processing in which a cryptographic key is renewed by using data resulting from an immediately preceding cryptographic processing. This reference does not teach performing a different key generation processing on each block. Our renewal of a key serves to improve the security level and/or reduce the computational load resulting from the key generation processing.

The Stallings Williams article discloses a technique to encrypt a plaintext block through *n* rounds of processing. Each round performs a round function F, an exclusive-OR, and a substitution of the left half and the right half of the data of the plaintext block. In each round function F, a different round subkey K_i is used. According to this technique, a number of different round subkeys K_i need to be generated every round, which leads to a problem that the encryption speed will be inevitably decreased.

The Charnes, et al. article discloses a technique to encrypt a plaintext block through 32 iterations. In each iteration, the data bits representing a plaintext is subjected to addition, conversion using S-boxes, bit rotation, exclusive-OR, and swapping of the high-order its and low-order bits. The above addition in each iteration is performed using a corresponding partial key that is derived from the same key. According to this technique, however, the same key is repeatedly used, and thus the security against malicious attacks is not maintained at a high level.

As recited in Claim 1, advantageous features of the present invention include a key generating step for generating

(1) a first group composed of a predetermined number *n* of different subkeys when the first mode is selected, and

(2) a second group composed of less than *n* different subkeys when the second

Received from < 949 955 2507 > at 6/27/03 3:02:19 PM [Eastern Daylight Time]

mode is selected.

Additionally, the present invention permits,

in the first mode, each of the *n* conversion processes to be associated with a different subkey in the first group and to be performed using the associated subkey, and

in the second mode, the *n* conversion processes are associated with subkeys in the second group and are each performed using the associated subkey.

According to the present invention, the above two modes are selectively used so that a high level of security is maintained against known plaintext attacks without greatly sacrificing encryption speed.

There is no teaching or suggestion of these in the Stallings Williams reference nor in the Charnes, et al. reference.

It is believed that all the requirements to have the present application made special have been complied with. if there are any questions or additional requirements, the undersigned attorney would appreciate a telephone conference.

I hereby certify that this correspondence is being transmitted via facsimile to Art Unit 2776, 703-308-6606, in the United States Patent and Trademark Office on June 27, 2003

By: Sharon Farnus

Signature

Date: June 27, 2003

Very truly yours,

SNELL & WILMER L.L.P.

Joseph W. Price
Registration No. 25,124
4920 Main Street, Suite 1200
Irvine, California 92614-7060
Telephone: (949) 253-4920

Received from < 949 955 2507 > at 6/27/03 3:02:19 PM [Eastern Daylight Time]

Snell & Wilmer
L.L.P.
LAW OFFICES

1920 Main Street, Suite 1200
Irvine, California 92614-7060

(949) 253-2700
Fax: (949) 955-2507
www.swlaw.com

IRVINE, CALIFORNIA
PHOENIX, ARIZONA
TUCSON, ARIZONA
SALT LAKE CITY, UTAH
DENVER, COLORADO
LAS VEGAS, NEVADA

FACSIMILE TRANSMISSION

DATE: June 27, 2003

TIME IN:
TIME OUT:

TO:

Name:	Fax Number:	Phone Number:
Art Unit 2776, USPTO	1-703-308-6606	

FROM: Joseph W. Price, Esq.
Reg. No.: 25,124

PHONE: 949-253-4920

MESSAGE:

Docket: 62478-1800 (BM08)
RE: 09/638,616

Dear Sirs:

Enclosed please find a corrected copy of the Petition to Make Special in the above application. Applicant submitted this Petition on June 24, 2003 via express mail. A clerical error was discovered in which the last sentence of Paragraph Two under REMARKS was incomplete. The enclosed copy includes the complete sentence. Kindly enter this corrected version of the Petition to Make Special. If you have any questions please do not hesitate to contact me.

Thank you.
Joseph W. Price

ORIGINAL DOCUMENT:

NUMBER OF PAGES (Including Cover): 5

CONFIRMATION NO.:

CLIENT MATTER NO.: 99999-0000

PLEASE RETURN TO:

PERSONAL FAX: No

REQUESTOR: Joseph W. Price

DIRECT LINE: 949-253-4920

**IF YOU HAVE NOT PROPERLY RECEIVED THIS TELECOPY, PLEASE CALL US AT (949) 253-2791.
OUR FACSIMILE NUMBER IS (949) 955-2507.**

THE INFORMATION CONTAINED IN THIS FACSIMILE MESSAGE IS ATTORNEY PRIVILEGED AND CONFIDENTIAL INFORMATION INTENDED ONLY FOR THE USE OF THE INDIVIDUAL OR ENTITY NAMED ABOVE. IF THE READER OF THIS MESSAGE IS NOT THE INTENDED RECIPIENT, OR THE EMPLOYEE OR AGENT RESPONSIBLE TO DELIVER IT TO THE INTENDED RECIPIENT, YOU ARE HEREBY NOTIFIED THAT ANY DISSEMINATION, DISTRIBUTION OR COPYING OF THIS COMMUNICATION IS STRICTLY PROHIBITED. IF YOU HAVE RECEIVED THIS COMMUNICATION IN ERROR, PLEASE IMMEDIATELY NOTIFY US BY TELEPHONE, AND RETURN THE ORIGINAL MESSAGE TO US AT THE ABOVE ADDRESS VIA THE U.S. POSTAL SERVICE. THANK YOU.

Received from < 949 955 2507 > at 6/27/03 3:02:19 PM [Eastern Daylight Time]